INFO:

Wikileaks a publié des milliers de documents qui révèlent les plus grands secrets de piratage de la CIA, qui incluent notamment la capacité de l'agence à pénétrer les systèmes d'exploitation iPhone, Android, Smart TV, Microsoft et Mac OS Linux.

10 choses à savoir sur les détournements du site Wikileaks des documents de la CIA

الحمدللَّه معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام على من أعلى اللَّه منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد

10 choses à savoir sur les détournements du site Wikileaks des documents de la CIA

Wikileaks a publié des milliers de documents qui révèlent les plus grands secrets de piratage de la CIA, qui incluent notamment la capacité de l'agence à pénétrer les systèmes d'exploitation iPhone, Android, Smart TV, Microsoft et Mac OS Linux.

Vault 7 n'est que la première partie de la série des détournements "**Year Zero**" don't Wikileaks fuira dans les prochains jours.

Vault7 est une operation de piratage mondiale subtile sur laquelle repose la **CIA.**

Selon **Whistleblower**, la **CIA** n'a pas averti les entreprises des problèmes de sécurité et des lacunes dans leurs produits, mais elle a conservé des vulnérabilités dans les systèmes d'exploitation, tels que les appareils Android, iPhone et téléviseurs intelligents.

L’un des documents divulgués était que la **CIA** cherchait des véhicules télécommandés avec des voitures et des camions intelligents, ce qui pourrait provoquer des "accidents" qui pourraient être efficaces pour des assassinats non traçables.

Alors que les experts en sécurité, les entreprises et les organisations à but non lucratif examinent toujours **8 761** documents divulgués, tels que les archives **Vault 7**, nous sommes ici avec quelques points et faits à connaître

Tout ce que vous devez savoir sur les fuites de Vault7:

- **WikiLeaks révèle les secrets de la CIA pour la piratage du telephone:**

La **CIA** a une liste éblouissante de façons de pirater votre téléphone Android, **iOS**, Windows Phone

Le **Vault7** comprend **8 761** documents et fichiers qui séparent les informations de renseignement des logiciels **CIA** sophistiqués pour pénétrer les smartphones ou les iPhones d’Apple d’Android, y compris sa capacité à contrôler entièrement les appareils.

En fait, Wikileaks affirme que la **CIA** dispose d’une unité de haut niveau dans la division du développement du téléphone, qui à son tour développe une vulnérabilité **zero-day** et un logiciel malveillant pour "infecter, contrôler et extraire les données **des iPhone** et autres appareils Apple **iOS** tels que les iPads".

Certaines attaques sont suffisamment puissantes pour permettre à un attaquant de capturer à distance sur “**nouwat kernel”**

Le cœur du système d'exploitation qui contrôle le fonctionnement du smartphone ou l'accès à la validité de la capacité “root” sur les appareils, permettant à l'attaquant d'accéder à des informations telles que l'emplacement, les contacts, les contacts, etc.

Ces types d'attaques sont utiles pour une pénétration intentionnelle ou dirigée, ainsi que pour une surveillance complete

Les fuites de documents ont également été séparées des attaques spécifiques que l'agence peut lancer sur certains smartphones et systèmes d'exploitation, y compris les versions récentes d'Android et d'**ios.**

- **La CIA n'a pas rompu le cryptage des applications, mais l'a dépassé**

La **CIA** a créé un logiciel malveillant capable de lire vos propres conversations sans casser le chiffrement

Des que les documents ayant été mis à disposition par Wikileaks, un malentendu a amené les gens à penser que la **CIA** avait "brisé" le cryptage utilisé par les programmes de messagerie sécurisés tels que Seqnal et Wattsapp

Wikileaks a confirmé que: Ces technologies permettent à la **CIA** de dépasser le cryptage **WhatsApp, Signal, Telegram, Wiebo, Confide** et **Cloakman** en pénétrant les périphériques "intelligents" sur lesquels elle fonctionne, et de mettre en commun la voix et les messages actuels avant leur cryptage.

Le rapport WikiLeaks a amené la plupart des gens à penser que le cryptage utilisé (**end-to-end**) par des clients de messagerie cryptés tels que **Signal** et **Whatsapp** a été rompu, non, ce n'était pas

Au lieu de cela, la **CIA** dispose d'outils lui permettant d'accéder à des téléphones entiers, ce qui évite bien sûr les applications de messagerie cryptées, car elle a éliminé tous les systèmes de sécurité artificiels du téléphone, donnant ainsi un accès à distance complet à l'agence.

Les documents WikiLeaks ne montre pas d'attaques spécifiques sur **Signal** ou **WhatsApp**, mais l'agence prend le contrôle de l'intégralité du téléphone et le surveille avant que les applications ne cryptent et n'envoient les informations.

Comme si vous étiez assis dans un train près de la cible et que vous lisiez sa conversation avec l'autre personne sur son téléphone ou son ordinateur portable pendant l'écriture, cela ne signifie pas que la sécurité de l'application utilisée par la cible présente des problèmes.

Dans ce cas, peu importe si les messages sont chiffrés pendant le transport si vous voyez tout ce qui se passe sur l'appareil avant toute mesure de sécurité.

Mais cela ne signifie pas que cela rend le problème plus facile, comme l'explique le client de dénonciation de la **NSA whistleblower** , Edward Snowden. «Cela montre à tort que la **CIA** a piraté le cryptage de ces applications, mais que Android et ios ont été pirates et c'est le grand probleme

- **La CIA développe des logiciels malveillants ciblant Windows, Linux, MacOS**

Wikileaks de la **CIA** comprend également des informations sur les logiciels malveillants pouvant être utilisés par l'agence pour pénétrer et espionner à distance et contrôler les ordinateurs fonctionnant sous **Windows, MacOS, Linux**.

Cela signifie que la **CIA** peut dépasser le chiffrement **PGP** et même le réseau privé virtuel (**VPN**) sur votre ordinateur de la même manière, et l'agence peut également voir tout ce que vous faites sur Internet, même si vous vous cachez derrière le navigateur Tor.

Cela ne signifie pas non plus que l'utilisation du navigateur **PGP, VPN** ou Tor n'est pas sécurisée ou que la **CIA** puisse pénétrer ces services, mais que la capacité de l'agence à pénétrer tout système d'exploitation pour prendre et contrôler complètement n'importe quel périphérique Ou un ordinateur portable ou une télévision avec un microphone - rend la **CIA** capable de dépasser tout service et d'espionner tout ce qui se passe sur l'appareil.

- **La CIA a emprunté des codes à partir d'échantillons génériques de logiciels malveillants**

La **CIA** utilise des échantillons de codes de logiciels malveillants disponibles au public pour adopter ses propres programmes d'espionnage

Oui, en plus des attaques présumées développées par la **CIA**, l'agence a adopté des codes provenant d'autres personnes, sources générales de logiciels malveillants

Un document mentionnait comment l'agence modifiait des fragments de code malveillant connus pour développer un code personnalisé et d'autres solutions ciblées.

"L'équipe **UMBRAGE** maintient une bibliothèque de technologies de développement d'applications empruntées aux logiciels malveillants" **in-the-wild** (dans la nature), comme indiqué dans le document de Wikileaks. "Le but de ce référentiel est de fournir des parties de code efficaces pouvant être rapidement mélangées dans des solutions personnalisées"

Certaines de ces caractéristiques ont été découvertes et publiées par des sociétés de sécurité, des groupes de pirates informatiques, des chercheurs indépendants, achetés ou acquis par la **CIA** auprès d'autres agences de renseignement telles que le **FBI**, la **NSA** et le **GCHQ**.

Une des fuites de "composants de destruction de données" inclut une référence à **Shamoon**, un logiciel malveillant capable de voler des données et d'analyser tout le disque dur.

SwampMonkey est une autre attaque de la **CIA**, qui permet à l'agence d'obtenir une validité "root" pour les appareils Android.

Un autre outil du référentiel d'armes de la **CIA** permet à l'agence de contrôler le périphérique cible chaque fois qu'il est reactive

- **La CIA a utilisé des applications avec des logiciels malveillants pour espionner les cibles**

(Fine Dining Attack) La **CIA** a utilisé des applications bombardées avec des logiciels malveillants pour espionner les cibles

Le document divulgué comprenait un fichier appelé "**Fine Dining**" qui ne contient pas des failles et des fuites **zero-day** , mais un ensemble d'applications exploitées avec un logiciel malveillant.

Fine Dining est une technologie hautement sophistiquée qui peut être largement déployée, comme dans le cas où la **CIA** attaque l'ordinateur

Les agents de terrain de la **CIA** conservent une ou plusieurs de ces applications, conformément à leurs objectifs, dans un périphérique de stockage externe **USB**, qu'ils font entrer dans les systèmes cibles pour qu'une application puisse le faire et collectent des données à partir du périphérique.

Mis au point par **OSB (Operational Support Branch**), qui est une division du centre de renseignements de l'Agence, **Fine Dining** contient des modules pouvant être utilisés pour encapsuler les applications suivantes:

VLC Player Portable

Irfanview

Chrome Portable

Opera Portable

Firefox Portable

ClamWin Portable

Kaspersky TDSS Killer Portable

McAfee Stinger Portable

Sophos Virus Removal

Thunderbird Portable

Opera Mail

Foxit Reader

LibreOffice Portable

Prezi

Babel Pad

Notepad++

Skype

Iperius Backup

Sandisk Secure Access

U3 Software

2048

LBreakout2

7-Zip Portable

Portable Linux CMD Prompt

- **Le déséspoir de la CIA de pirater le cryptage d'Apple**

La **CIA** travaille dur depuis des années pour briser le cryptage d'Apple

Ce n'est pas la première fois que la **CIA** essaie de cibler les appareils de la **IOS**, il a été mentionné précédemment que la **CIA** a ciblé des appareils Apple (**iPhone - iPad**), et ne divulgation très secrète du système wiki interne de l'Agence suit les fuites de Snodden en **2015**

Les documents ont montré que la **CIA** visait les clés de sécurité de base utilisées pour chiffrer les données stockées dans les appareils Apple utilisant à la fois **physical** et **non invasive**, ainsi que les techniques de la **CIA**, Département de pirater pour le **FBI (Unité des opérations à distance - Remote Operations Unit**) qui travaillait aussi désespérément à découvrir les lacunes dans les dispositifs de l'**iPhone**, comme l'indique l'un des documents de WikiLeaks, qui peut également être la raison derrière la quête de l'agence pour forcer Apple à développer une échappatoire efficace pour pénétrer le contenu de l'iPhone d'un de mes attaquants San Bernardino.

- **Apple affirme avoir réparé plusieurs des lacunes révélées par les fuites de la CIA**

À côté des lacunes dans les téléviseurs intelligents Android et Samsung

Des fuites de documents détaillent **14** lacunes dans l'**IOS**, décrivant comment l'agence utilise ces problèmes de sécurité pour suivre les utilisateurs, surveiller leurs contacts et même contrôler complètement leurs téléphones.

Quoi qu'il en soit, Apple nie les allégations selon lesquelles la **CIA** aurait enregistré des erreurs de logiciel car ses machines sont efficaces.

Selon Apple, de nombreuses lacunes dans le conteneur WikiLeaks de **CIA** ont déjà été corrigées dans la dernière version d'**iOS** publiée en janvier, tandis que les ingénieurs Apple continuent de travailler pour résoudre les nouvelles failles connues de la **CIA**.

Ceci est une déclaration soumise par le porte-parole officiel d'Apple:

« Apple est pleinement engagé à la protection de la vie privée de la sécurité" la technologie des utilisateurs fait à l'intérieur de l'iPhone aujourd'hui offre aux consommateurs la meilleure protection disponible pour les données, et nous travaillons en permanence pour maintenir de cette façon, nos produits et systèmes conçus pour obtenir rapidement des mises à jour de sécurité jusqu'à les mains des utilisateurs, avec environ **80%** des les utilisateurs disposent des dernières versions des systèmes d'exploitation, alors que l'analyse initiale indique que bon nombre des problèmes divulgués aujourd'hui ont déjà été corrigés dans la dernière version d'**iOS**, nous allons continuer à travailler rapidement pour corriger les faiblesses qui ont été identifiées, nous demandons instamment toujours aux utilisateurs de télécharger la dernière version d'**iOS** pour vous assurer Les obtenir les dernières mises à jour de sécurité "

- **Le piratage de toute personne n'importe où grâce l'à Internet peu sûr**

La **CIA** peut pénétrer votre smart TV et d'autres appareils intelligents pour vous espionner

Outre des centaines d'échappatoires, de «**zero days**» et de pirates informatiques visant un grand nombre de systèmes et de services, **Vault7** présente également des détails sur **codenamed Weeping Angel** - utilisé par la **CIA** pour pénétrer les téléviseurs intelligents.

Les téléviseurs intelligents de Samsung sont vulnérables à la pénétration de appareils, ce qui rend la télévision en mode fermé.L'utilisateur pense que la télévision est fermée mais elle est est ouverte, permettant à la **CIA** d'enregistrer secrètement les conversations dans la salle et de les envoyer a travers Internet à un serveur secret de la **CIA Weeping Angel,** l'appui des boutons du remote s'arrete ou le televiseur sera en veille prolongée pour que le systeme entre dans un faux verrou et "le document fuit" indique que **l'implant** est deja à l'origine de ces evenements, l'**implant** sait quand le téléviseur passé ewn mode de verouillage erroné**.**

En réponse au document de Wikileaks pour la **CIA**, Samsung a publié une déclaration disant: "Protection du consommateur" La confidentialité et la sécurité de nos appareils sont la priorité absolue chez Samsung, nous sommes au courant du rapport et nous le regardons rapidement

- **Les fuites de Wikileaks pour la CIA ne sont pas plus grandes que celles de SNODIN**

La **CIA** n'est pas plus avancée que l'équipe **TAO** de la **NSA** et les fuites de **Vault7** ne sont même pas supérieures aux fuites de Snowden

WikiLeaks affirme que les fuites de piratage majeures de la **CIA** sont plus importantes que celles d'Edward Snowden sur les mesures de répression et les programmes de censure de la **NSA**, mais elles sont très similaires

Alors que Snodin a révélé une surveillance secrète mondiale via des messages texte et la voix de personnes utilisant des outils révolutionnaires permettant de collecter et d'analyser de grandes quantités de données le conteneur de données de la **CIA** est très profond, ce qui montre que la collecte et l'approvisionnement en outils de la **CIA** peuvent être utilisés pour cibler des périphériques individuels.

Cependant, il n'y a pas de preuve de contrôle global sur les téléphones intelligents ou les ordinateurs dans les documents divulgués: techniquement, la **NSA** possède plus d'expertise technique et est plus sophistiquée que Kia.

- **L'ancien chef de la CIA a déclaré que le conteneur WikiLeaks avait rendu les États-Unis moins sûrs**

L’ancien chef de la **CIA** affirme que les fichiers de la **CIA** divulgués par Wikileaks sont très dommageables et mettent un danger

L'ancien chef de la **CIA**, Michael Hayden, a déclaré que les fuites récentes de documents et de dossiers de la **CIA** très sensibles de WikiLeaks étaient "très dommageables" et menaçaient, le rapport de la **BBC**, bien que la **CIA** n'ait pas encore commenté sur les fuites

La découverte de **la CIA** par les dénonciateurs de **whistleblower** en est encore à ses balbutiements, les gens verront de plus en plus de fuites concernant le gouvernement et les agences de Wikileaks dans les prochains jours dans le cadre de leurs fuites «**Year Zero**».

****

Horizons

مؤسسة آفاق الإلكترونية

للتواصل:

@EHFTS

@SR444TAW

جميع حقوق النشر محفوظة لدى مؤسسة آفاق الإلكترونية 2018 ©
ولانبيح نسخ المواد العلمية والأمنية التى تقدمها المؤسسة دون ذكر المصدر